

Repair Locality From a Combinatorial Perspective

Anyu Wang and Zhifang Zhang

Key Laboratory of Mathematics Mechanization, NCMIS

Academy of Mathematics and Systems Science, Chinese Academy of Sciences

Beijing, 100190

Email: wanganyu@amss.ac.cn, zfz@amss.ac.cn

Abstract

Repair locality is a desirable property for erasure codes in distributed storage systems. Recently, different structures of local repair groups have been proposed in the definitions of repair locality. In this paper, the concept of *regenerating set* is introduced to characterize the local repair groups. A definition of locality $r^{(\delta-1)}$ (i.e., locality r with repair tolerance $\delta - 1$) under the most general structure of regenerating sets is given. All previously studied locality turns out to be special cases of this definition. Furthermore, three representative concepts of locality proposed before are reinvestigated under the framework of regenerating sets, and their respective upper bounds on the minimum distance are reproved in a uniform and brief form. Additionally, a more precise distance bound is derived for the *square code* which is a class of linear codes with locality $r^{(2)}$ and high information rate, and an explicit code construction attaining the optimal distance bound is obtained.

I. INTRODUCTION

In modern large-scale storage systems, erasure codes can afford higher data reliability with considerably smaller storage overhead [15]. An important issue in utilizing erasure codes is data repair in case of node failures so that the whole storage system keeps the same level of redundancy. Nevertheless how to reduce the repair cost becomes a key problem that affects the practical applications of erasure codes. There are several cost metrics that can be optimized during the repair process: the repair bandwidth [1], i.e., the total number of bits communicated in the network, the number of bits read from existing disks [13], and the repair locality [2], [4], i.e., the number of nodes that participate in the repair process. Each of these metrics is relevant to different application environments. For cloud storage applications, the main performance bottleneck is the disk I/O [4], which is proportional to the number of nodes connected during the repair process.

A related performance metric is *repair locality* which was first introduced for linear scalar codes [2], [7]. Specifically, a coordinate of a linear scalar code has locality r if the value at this coordinate can be recovered by a linear combination of the values at r other coordinates. We say these r coordinates form a *local repair group* of the former coordinate. Then in [9] the locality r was generalized to vector and nonlinear codes while the structure of local repair groups remained unchanged. Later, the structure of error-correcting codes was adopted in local repair groups, which gave the definition of locality (r, δ) in [10]. Since the local repair group provides a subcode with minimum distance δ , the locality (r, δ) can tolerate up to $\delta - 1$ erasures, which means even when $\delta - 1$ nodes fail in the system, each failed node can still be repaired by accessing r existing nodes. This locality was also generalized to vector and nonlinear codes in [11]. Recently, another kind of locality with $(\delta - 1)$ -erasure tolerance has been proposed as the $(r, \delta)_c$ -locality [14], where the local repair group consists of $\delta - 1$ disjoint subsets. This new structure of local repair groups leads to an improvement in the minimum distance. With all these definitions of locality, the upper bounds on the minimum distance were derived respectively, and codes attaining the upper bounds were constructed.

In this paper, we introduce the concept of *regenerating set* to characterize the local repair groups. Under the framework of regenerating sets, we develop a uniform approach to analyze the minimum code distance for different kinds of locality. Specifically, a connection between the minimum distance and the

Table 1

locality	α	linear / nonlinear	δ	local repair group
[2]: locality r	$\alpha = 1$	linear	$\delta = 2$	single subset
[9]: $C(n, r, d, \alpha)$ codes	$\alpha \geq 1$	both	$\delta = 2$	single subset
[10]: locality (r, δ)	$\alpha = 1$	linear	$\delta \geq 2$	error correcting codes
[11]: (r, δ, α) codes	$\alpha \geq 1$	both	$\delta \geq 2$	error correcting codes
[14]: $(r, \delta)_c$ -locality	$\alpha = 1$	linear	$\delta \geq 2$	disjoint repair sets
[8]: repair tolerance $\delta(i)$	$\alpha = 1$	linear	$\delta \geq 2$	general
this paper: locality $r^{\delta-1}$	$\alpha \geq 1$	both	$\delta \geq 2$	general

regenerating set structure is established for any code, so the problem of estimating the code distance is transformed into calculating the size of unions of regenerating sets, and the latter is a simple combinatorial problem. In detail, this paper includes three contributions that benefit from the framework of regenerating sets.

- (1) *The most general definition.* We define the locality $r^{(\delta-1)}$ to describe the locality r along with repair tolerance $\delta - 1$ under a general structure of local repair groups. The definition applies to both linear and nonlinear codes. All previously studied locality are actually special cases of this definition.
- (2) *Uniform and brief proofs.* We reinvestigate three representative families of codes with different locality proposed before, and reprove the upper bounds of the minimum distance in a combinatorial way. The proofs present an uniform and brief form.
- (3) *Precise bound.* We derive an upper bound on the minimum distance for a class of specific codes. This bound turns out to be more precise than that given before [14]. Moreover, we present an explicit code construction that attains this upper bound.

A. Related Work

As we have stated, previously proposed locality all fall into the scope of our locality $r^{(\delta-1)}$. Table 1 gives a comparison of different definitions of locality, where α stands for the size of each coded fragment, namely, $\alpha = 1$ means the locality only applies to scalar codes while $\alpha \geq 1$ means it also applies to vector codes, and δ denotes the repair tolerance.

The framework of regenerating sets proposed in this paper extends the matroid approach used in [12] to the vector case and nonlinear case. Particularly, it is sufficient for paper [12] to study circuits in linear matroids because only linear scalar codes were concerned there. However, because of generalization of the locality $r^{(\delta-1)}$ in this paper we alternatively define the regenerating set to characterize local repair groups, and develop effective approaches accordingly to prove the code distance bound.

B. Organization

Section II introduces the concept of regenerating set and shows its connection with the minimum distance. Section III gives the definition of locality $r^{(\delta-1)}$ and reproves the upper bounds of code distance for three kinds of locality proposed before. Section IV derives an upper code distance bound for the square codes and an explicit construction attaining this bound. Section V concludes the paper.

II. REGENERATING SETS AND THE MINIMUM DISTANCE

Let G be an encoding function that takes input a file of size M over an alphabet Σ and outputs n coded fragments of size α over Σ , that is,

$$G(X) = (Y_1, \dots, Y_n),$$

where $X \in \Sigma^M$ and $Y_i \in \Sigma^\alpha$ for $i = 1, \dots, n$. Note that X can be viewed as a random variable which is uniformly drawn from Σ^M and Y_1, \dots, Y_n are random variables over Σ^α . Namely, $H(X) = M$ and

$H(Y_i) \leq \alpha$, where $H(\cdot)$ is the $|\Sigma|$ -ary entropy function. For convenience, we denote the code determined by the encoding function G as an $(n, (M, \alpha), d)$ code \mathcal{C} , where d is the minimum distance defined as follows:

Definition 1. *The minimum distance of \mathcal{C} is defined as*

$$d = n - \max\{|E| : E \subseteq [n] \text{ and } H(Y_E) < M\},$$

where $[n]$ denotes the set of integers $\{1, 2, \dots, n\}$ and Y_E is the set of random variables $\{Y_i\}_{i \in E}$.

It follows from the definition that any $n - d + 1$ of the variables Y_1, Y_2, \dots, Y_n have joint entropy M , and therefore the $(n, (M, \alpha), d)$ code \mathcal{C} can tolerate up to $d - 1$ erasures. To ensure the repair of all coordinates, we assume $d \geq 2$ throughout the paper. A trivial result is that $H(Y_1, \dots, Y_n) = M$.

A. Regenerating Sets

Now we define the regenerating set with respect to an $(n, (M, \alpha), d)$ code \mathcal{C} .

Definition 2. *For any $i \in [n]$, a regenerating set of the i -th coordinate is a subset $R \subseteq [n]$ satisfying $i \in R$ and $H(Y_i | Y_{R \setminus \{i\}}) = 0$.*

It can be seen that any coordinate of \mathcal{C} has at least one regenerating set when the minimum distance $d \geq 2$. Moreover, if R is a regenerating set of the i -th coordinate, then any set R' satisfying $R \subseteq R' \subseteq [n]$ is also a regenerating set of the i -th coordinate. We denote the collection of all regenerating sets of the i -th coordinate as \mathcal{R}_i .

Definition 3. *A sequence of regenerating sets R_1, R_2, \dots, R_m , where $R_i \in \mathcal{R}_{l_i}$ for $1 \leq i \leq m$ and $l_i \in [n]$, is said to have a nontrivial union if $l_j \notin \cup_{i=1}^{j-1} R_i$ for $1 \leq j \leq m$.*

The structure of nontrivial union plays an important role in estimating the minimum distance of a code. The following proposition gives an upper bound on the entropy of a nontrivial union of regenerating sets in terms of its set size.

Proposition 1. *Suppose a sequence of regenerating sets R_1, R_2, \dots, R_m has a nontrivial union, where $R_i \in \mathcal{R}_{l_i}$ and $l_i \in [n]$ for $1 \leq i \leq m$. Then $H(Y_{\cup_{i=1}^m R_i}) \leq \alpha(|\cup_{i=1}^m R_i| - m)$.*

Proof: We prove this by induction on m . First for $m = 1$,

$$\begin{aligned} H(Y_{R_1}) &= H(Y_{R_1 \setminus \{l_1\}}) + H(Y_{l_1} | Y_{R_1 \setminus \{l_1\}}) \\ &= H(Y_{R_1 \setminus \{l_1\}}) \\ &\leq \alpha(|R_1| - 1). \end{aligned}$$

Then suppose the argument holds for $m - 1$, where $m > 1$. Let $R_m = \{l_m\} \cup A \cup B$ be a partition of R_m such that $A \subseteq \cup_{i=1}^{m-1} R_i$ and $B \cap (\cup_{i=1}^{m-1} R_i) = \emptyset$. Because $H(Y_{l_m} | Y_{A \cup B}) = 0$ and $A \subseteq \cup_{i=1}^{m-1} R_i$, it has

$$\begin{aligned} H(Y_{\cup_{i=1}^m R_i}) &= H(Y_{\cup_{i=1}^{m-1} R_i}, Y_B) \\ &\leq H(Y_{\cup_{i=1}^{m-1} R_i}) + H(Y_B) \\ &\leq \alpha(|\cup_{i=1}^{m-1} R_i| - (m - 1)) + \alpha|B| \\ &= \alpha(|\cup_{i=1}^m R_i| - m), \end{aligned}$$

where the last equality comes from the definition of nontrivial union and the partition of R_m . ■

B. Upper Bound of the Minimum Distance

We continue to define some notations with respect to an $(n, (M, \alpha), d)$ code and derive an upper bound of d . First, define a function $\Phi(x)$ to be the minimum size of a nontrivial union of x regenerating sets,

$$\text{i.e., } \Phi(x) = \min\{|\cup_{i=1}^x R_i| : R_i \in \mathcal{R}_{l_i} \text{ and } R_1, \dots, R_x \text{ have a nontrivial union}\}.$$

In particular, we assume $\Phi(0) = 0$. It is easy to see $\Phi(x+1) \geq \Phi(x) + 1$, thus $\Phi(x) - x$ is an increasing function with respect to x .

Define

$$\rho = \max\{x \mid \Phi(x) - x < \frac{M}{\alpha}\}.$$

Obviously, $\rho \geq 0$. The next is a corollary of Proposition 1.

Corollary 1. For $0 \leq x \leq \rho$, let $R_1^{(x)}, R_2^{(x)}, \dots, R_x^{(x)}$ be a sequence of regenerating sets that has a nontrivial union and $\Phi(x) = |\cup_{i=1}^x R_i^{(x)}|$. Then $[n] - \cup_{i=1}^x R_i^{(x)} \neq \emptyset$.

Proof: By Proposition 1,

$$\begin{aligned} H(Y_{\cup_{i=1}^x R_i^{(x)}}) &\leq \alpha(|\cup_{i=1}^x R_i^{(x)}| - x) \\ &= \alpha(\Phi(x) - x) \\ &\leq \alpha(\Phi(\rho) - \rho) \\ &< M. \end{aligned}$$

Since $H(Y_1, \dots, Y_n) = M$, then $[n] - \cup_{i=1}^x R_i^{(x)} \neq \emptyset$. ■

Theorem 1. Let \mathcal{C} be an $(n, (M, \alpha), d)$ code, then

$$d \leq n - \lceil \frac{M}{\alpha} \rceil + 1 - \rho.$$

Proof: Without loss of generality, suppose $\Phi(\rho) = |\cup_{i=1}^\rho R_i|$, where $R_i \in \mathcal{R}_{l_i}$ and R_1, \dots, R_ρ have a nontrivial union. Then

$$|\cup_{i=1}^\rho R_i| = \Phi(\rho) \leq \rho + \lceil \frac{M}{\alpha} \rceil - 1$$

by the definition of ρ . From Corollary 1, $[n] - \cup_{i=1}^\rho R_i \neq \emptyset$. Furthermore, for any set $T \subseteq [n] - \cup_{i=1}^\rho R_i$ with $|T \cup (\cup_{i=1}^\rho R_i)| \leq \rho + \lceil \frac{M}{\alpha} \rceil - 1$, we have

$$\begin{aligned} H(Y_{(\cup_{i=1}^\rho R_i) \cup T}) &\leq H(Y_{\cup_{i=1}^\rho R_i}) + H(Y_T) \\ &\leq \alpha(|\cup_{i=1}^\rho R_i| - \rho) + \alpha|T| \\ &= \alpha(|(\cup_{i=1}^\rho R_i) \cup T| - \rho) \\ &\leq \alpha(\lceil \frac{M}{\alpha} \rceil - 1) \\ &< M. \end{aligned}$$

Particularly, choose a set $T' \subseteq [n] - \cup_{i=1}^\rho R_i$ with $|T' \cup (\cup_{i=1}^\rho R_i)| = \rho + \lceil \frac{M}{\alpha} \rceil - 1$, then $H(Y_{(\cup_{i=1}^\rho R_i) \cup T'}) < M$. Thus by Definition 1, $d \leq n - |(\cup_{i=1}^\rho R_i) \cup T'| = n - \lceil \frac{M}{\alpha} \rceil + 1 - \rho$. ■

From the theorem, upper-bounding the minimum distance mainly depends on computing the value of ρ which in turn relies on computation of the function $\Phi(x)$.

III. CODES WITH LOCALITY

Next we give the general definition of locality. It can be regarded as an extension of the repair tolerance defined in [8] to include the vector case and the nonlinear case.

Definition 4. Let \mathcal{C} be an $(n, (M, \alpha), d)$ code. For $i \in [n]$, we say the i -th coordinate of \mathcal{C} has locality r with repair tolerance $\delta - 1$, denoted as locality $r^{(\delta-1)}$, if for all subset $E \subseteq [n]$ containing i with $|E| \leq \delta - 1$, there exists a regenerating set $R \in \mathcal{R}_i$ such that

- (1) $|R| \leq r + 1$, and
- (2) $R \cap E = \{i\}$.

That is, a coordinate of \mathcal{C} has locality $r^{(\delta-1)}$ if for any codeword of \mathcal{C} , the value at this coordinate can be regenerated by accessing at most r other coordinates even in the presence of any other $\delta - 2$ erasures. The generalization of our definition of locality $r^{(\delta-1)}$ is twofold. When $\delta = 2$, it coincides with the repair locality r defined for vector codes in [9], and certainly coincides with the repair locality r in [2] if we further restrict \mathcal{C} to a linear scalar code. When $\delta > 2$, the definition of locality $r^{(\delta-1)}$ describes the repair tolerance of $\delta - 1$ erasures in the most general way, instead of specifying the structure of local repair groups that provides the $(\delta - 1)$ -erasure tolerance. Therefore, the locality defined in [10], [11] by using inner-error-correcting code and that in [14] by using disjoint repair sets both fall into the scope of our definition. We call an $(n, (M, \alpha), d)$ code \mathcal{C} has locality $r^{(\delta-1)}$ if for all $i \in [n]$ the i -th coordinate of \mathcal{C} has locality $r^{(\delta-1)}$.

In the following we reinvestigate some previously studied locality from a combinatorial perspective. Namely, we describe the locality by specifying the structure of their regenerating sets and upper-bound the minimum distance by estimating the size of some set unions.

A. The Code $\mathcal{C}(n, r, d, \alpha)$

As defined in [9] the i -th coordinate of a code has repair locality r if the value at this coordinate is a function of values at r other coordinates. The notation $\mathcal{C}(n, r, d, \alpha)$ is used there to denote a code with all symbol locality r . By using the concept of regenerating sets, the code $\mathcal{C}(n, r, d, \alpha)$ is an $(n, (M, \alpha), d)$ code satisfying that for all $i \in [n]$ there exists a set $R_i \in \mathcal{R}_i$ with $|R_i| \leq r + 1$.

Lemma 1. For a code $\mathcal{C}(n, r, d, \alpha)$, it holds that $\Phi(x) \leq (r + 1)x$, where $0 \leq x \leq \rho + 1$.

Proof: We prove this lemma by induction on x . Because $\Phi(0) = 0$, the lemma trivially holds for $x = 0$. Assume it holds for x , where $x \leq \rho$. Let T_x be the union of a sequence of x regenerating sets that has a nontrivial union and $\Phi(x) = |T_x| \leq (r + 1)x$. From Corollary 1, $[n] - T_x \neq \emptyset$. It follows that there exists $h \in [n] - T_x$ and $R \in \mathcal{R}_h$ with $|R| \leq r + 1$, therefore

$$\begin{aligned} \Phi(x + 1) &\leq |T_x \cup R| \\ &\leq |T_x| + |R| \\ &\leq (r + 1)(x + 1). \end{aligned}$$

■

Theorem 2. For a code $\mathcal{C}(n, r, d, \alpha)$, it has

$$d \leq n - \lceil \frac{M}{\alpha} \rceil - \lceil \frac{M}{r\alpha} \rceil + 2.$$

Proof: By the definition of ρ , $\frac{M}{\alpha} \leq \Phi(\rho + 1) - (\rho + 1)$, and $\Phi(\rho + 1) \leq (r + 1)(\rho + 1)$ from Lemma 1. It follows that

$$\begin{aligned} \frac{M}{\alpha} &\leq \Phi(\rho + 1) - (\rho + 1) \\ &\leq (r + 1)(\rho + 1) - (\rho + 1) \\ &= r(\rho + 1), \end{aligned}$$

and therefore $\rho \geq \lceil \frac{M}{r\alpha} \rceil - 1$. Consequently, $d \leq n - \lceil \frac{M}{\alpha} \rceil - \lceil \frac{M}{r\alpha} \rceil + 2$ by Theorem 1. \blacksquare

B. The (n, r, δ, α) Locally Repairable Code

The (n, r, δ, α) locally repairable code defined in [11] is a generalization of the (r, δ) locality which was first proposed in [2]. This locality is due to a subcode of length no more than $r + \delta - 1$ and minimum distance at least δ . In other words, an (n, r, δ, α) locally repairable code is an $(n, (M, \alpha), d)$ code such that for $1 \leq i \leq n$, there exists a subset $S_i \subseteq [n]$ satisfying

- (1) $i \in S_i$, $\delta \leq |S_i| \leq r + \delta - 1$; and
- (2) For any $E \subseteq S_i$ with $|E| = \delta - 1$, and for any $j \in E$, it has $(S_i - E) \cup \{j\} \in \mathcal{R}_j$.

Lemma 2. For an (n, r, δ, α) locally repairable code, it holds that $\Phi(x) \leq r \lceil \frac{x}{\delta-1} \rceil + x$, where $0 \leq x \leq \rho + 1$.

Proof: We prove this lemma by induction on x . First, it trivially holds for $x = 0$. Suppose it holds for $x \leq x_0$, where $0 \leq x_0 \leq \rho$. Denote $x_0 + 1 = a(\delta - 1) + b$ where $a \in \mathbb{Z}$ and $b \in [\delta - 1]$. Let $T_{a(\delta-1)} = R_1 \cup \dots \cup R_{a(\delta-1)}$ be a nontrivial union of $a(\delta - 1)$ regenerating sets such that $\Phi(a(\delta - 1)) = |T_{a(\delta-1)}|$. There are two cases:

(1) There exists $h \in [n] - T_{a(\delta-1)}$ such that $|S_h - T_{a(\delta-1)}| \geq \delta - 1$, where the notation S_h comes from the description before this lemma. Choose $E \subseteq S_h - T_{a(\delta-1)}$ with $|E| = \delta - 1$. Suppose $E = \{i_1, \dots, i_{\delta-1}\}$. Let $R_{i_j} = (S_h - E) \cup \{i_j\}$ for $j \in [\delta - 1]$. Then $R_{i_j} \in \mathcal{R}_{i_j}$ and $(\cup_{j=1}^{a(\delta-1)} R_j) \cup (\cup_{j=1}^b R_{i_j})$ is a nontrivial union. It follows that

$$\begin{aligned} \Phi(x_0 + 1) &\leq |T_{a(\delta-1)} \cup R_{i_1} \cup \dots \cup R_{i_b}| \\ &\leq \Phi(a(\delta - 1)) + |S_h - E| + b \\ &\leq ar + a(\delta - 1) + r + b \\ &= r \lceil \frac{x_0 + 1}{\delta - 1} \rceil + x_0 + 1. \end{aligned}$$

(2) For any $h \in [n] - T_{a(\delta-1)}$, $|S_h - T_{a(\delta-1)}| < \delta - 1$. Define $R_h = (S_h \cap T_{a(\delta-1)}) \cup \{h\}$, then $R_h \in \mathcal{R}_h$. If $n - |T_{a(\delta-1)}| \geq b$, then choose $h_1, \dots, h_b \in [n] - T_{a(\delta-1)}$. So

$$\begin{aligned} \Phi(x_0 + 1) &\leq |T_{a(\delta-1)} \cup R_{h_1} \cup \dots \cup R_{h_b}| \\ &= |T_{a(\delta-1)}| + b \\ &= \Phi(a(\delta - 1)) + b \\ &\leq r \lceil \frac{x_0 + 1}{\delta - 1} \rceil + x_0 + 1. \end{aligned}$$

If $n - |T_{a(\delta-1)}| < b$, then

$$\Phi(x_0 + 1) \leq n < |T_{a(\delta-1)}| + b \leq r \lceil \frac{x_0 + 1}{\delta - 1} \rceil + x_0 + 1. \quad \blacksquare$$

Theorem 3. For an (n, r, δ, α) locally repairable code, it has

$$d \leq n - \lceil \frac{M}{\alpha} \rceil + 1 - (\lceil \frac{M}{r\alpha} \rceil - 1)(\delta - 1).$$

Proof: Similar to the proof of Theorem 2, we have

$$\frac{M}{\alpha} \leq \Phi(\rho + 1) - (\rho + 1) \leq r \lceil \frac{\rho + 1}{\delta - 1} \rceil.$$

It follows that $\lceil \frac{M}{r\alpha} \rceil \leq \lceil \frac{\rho + 1}{\delta - 1} \rceil$, and therefore $(\lceil \frac{M}{r\alpha} \rceil - 1)(\delta - 1) \leq (\lceil \frac{\rho + 1}{\delta - 1} \rceil - 1)(\delta - 1) \leq \rho$. Then Theorem 1 gives the desired bound. \blacksquare

C. The $(r, \delta)_c$ -Locality

An $(n, (M, \alpha), d)$ code has $(r, \delta)_c$ -locality if for $1 \leq i \leq n$, there exist $R_{i,1}, R_{i,2}, \dots, R_{i,\delta-1} \in \mathcal{R}_i$ satisfying

- (1) $|R_{i,j}| \leq r + 1$ for $1 \leq j \leq \delta - 1$; and
- (2) $R_{i,j} \cap R_{i,j'} = \{i\}$ for $1 \leq j \neq j' \leq \delta - 1$.

Paper [14] considered the $(r, \delta)_c$ -locality only for the linear scalar case, so in the following we set $\alpha = 1$ and consider linear codes.

Lemma 3. *For a linear $(n, (M, 1), d)$ code with $(r, \delta)_c$ -locality, it holds $\Phi(x) \leq rx + \lceil \frac{x}{\delta-1} \rceil$ where $0 \leq x \leq \rho + 1$.*

Proof: This lemma is proved by induction on x . First, it trivially holds for $x = 0$. Suppose it holds for $x \leq x_0$, where $0 \leq x_0 \leq \rho$. Denote $x_0 + 1 = a(\delta - 1) + b$ where $a \in \mathbb{Z}$ and $b \in [\delta - 1]$. Let $T_{a(\delta-1)} = R_1 \cup \dots \cup R_{a(\delta-1)}$ be a nontrivial union of $a(\delta - 1)$ regenerating sets such that $\Phi(a(\delta - 1)) = |T_{a(\delta-1)}|$. There are two cases:

(1) There exists $h \in [n] - T_{a(\delta-1)}$ such that $R_{h,j} \cap T_{a(\delta-1)} = \emptyset$ for $j \in [\delta - 1]$. Because of linearity, for $1 \leq j \leq \delta - 1$, there exists $i_j \in R_{h,j} - \{h\}$ such that $R_{h,j} \in \mathcal{R}_{i_j}$. Then $T_{a(\delta-1)} \cup R_{h,1} \cup \dots \cup R_{h,b}$ is a nontrivial union. It follows that

$$\begin{aligned} \Phi(x_0 + 1) &\leq |T_{a(\delta-1)} \cup R_{h,1} \cup \dots \cup R_{h,b}| \\ &\leq \Phi(a(\delta - 1)) + |R_{h,1} \cup \dots \cup R_{h,b}| \\ &\leq ra(\delta - 1) + a + rb + 1 \\ &= r(x_0 + 1) + \lceil \frac{x_0 + 1}{\delta - 1} \rceil. \end{aligned}$$

(2) For any $h \in [n] - T_{a(\delta-1)}$, there exists $j_h \in [\delta - 1]$ such that $R_{h,j_h} \cap T_{a(\delta-1)} \neq \emptyset$. If $n \geq |T_{a(\delta-1)}| + br$, then there exists h_1, \dots, h_b such that

$$h_l \in [n] - (T_{a(\delta-1)} \cup R_{h_1,j_{h_1}} \cup \dots \cup R_{h_{l-1},j_{h_{l-1}}}), \text{ for } 1 \leq l \leq b$$

because $|T_{a(\delta-1)} \cup R_{h_1,j_{h_1}} \cup \dots \cup R_{h_{l-1},j_{h_{l-1}}}| \leq |T_{a(\delta-1)}| + (l - 1)r < n$. Therefore $R_{h,j_h} \in \mathcal{R}_h$ for $h \in \{h_1, \dots, h_b\}$ and $T_{a(\delta-1)} \cup R_{h_1,j_{h_1}} \cup \dots \cup R_{h_b,j_{h_b}}$ is a nontrivial union. It follows that

$$\begin{aligned} \Phi(x_0 + 1) &\leq |T_{a(\delta-1)} \cup R_{h_1,j_{h_1}} \cup \dots \cup R_{h_b,j_{h_b}}| \\ &\leq |T_{a(\delta-1)}| + rb \\ &\leq ra(\delta - 1) + a + rb \\ &< r(x_0 + 1) + \lceil \frac{x_0 + 1}{\delta - 1} \rceil. \end{aligned}$$

If $n < |T_{a(\delta-1)}| + br$, then

$$\begin{aligned} \Phi(x_0 + 1) &\leq n < |T_{a(\delta-1)}| + rb \\ &< r(x_0 + 1) + \lceil \frac{x_0 + 1}{\delta - 1} \rceil. \end{aligned}$$

■

Theorem 4. *For a linear $(n, (M, 1), d)$ code with $(r, \delta)_c$ -locality, it has*

$$d \leq n - M + 1 - \mu,$$

where $\mu = \lceil \frac{(M-1)(\delta-1)+1}{(r-1)(\delta-1)+1} \rceil - 1$.

Proof: By Lemma 3 and the maximality of ρ ,

$$\begin{aligned}
M &\leq \Phi(\rho + 1) - (\rho + 1) \\
&\leq (r - 1)(\rho + 1) + \lceil \frac{\rho + 1}{\delta - 1} \rceil \\
&\leq (r - 1)(\rho + 1) + \frac{\rho}{\delta - 1} + 1.
\end{aligned}$$

It follows that $\rho \geq \lceil \frac{(M-1)(\delta-1)+1}{(r-1)(\delta-1)+1} \rceil - 1$. Then Theorem 1 gives the desired bound. \blacksquare

IV. THE SQUARE CODE

For explicit code constructions, especially when the structure of regenerating sets is given, Theorem 1 can be used to give more precise characterization of the minimum distance. For instance, in this section we utilize Theorem 1 to derive a tight bound on the minimum distance of the square code which was introduced in [14] as a class of code with $(r, \delta)_c$ -locality, a special case of the locality $r^{(\delta-1)}$. Besides the property of repair tolerance $\delta = 3$ for all coordinates, the square code also has the following advantage.

- (1) High information rate. Some square codes have information rate close to 1.
- (2) Desirable code distance. It was shown in [14], under the same level of local repair tolerance and information rate, the square code has the minimum distance beyond the upper bound for the (r, δ) locality defined in [10].

We first restate the square code as a linear $(n, (M, 1), d)$ code over \mathbb{F}_q , where $n = (r+1)^2$, $r+1 \leq M \leq r^2$ and its generator matrix $G = (x_{i,j})_{1 \leq i,j \leq r+1}$ is composed of n column vectors $x_{i,j} \in \mathbb{F}_q^M$ satisfying

$$\begin{cases} \sum_{i=1}^{r+1} x_{i,j} = 0, & \text{for } 1 \leq j \leq r+1 \\ \sum_{j=1}^{r+1} x_{i,j} = 0, & \text{for } 1 \leq i \leq r+1. \end{cases} \quad (1)$$

There is a grid corresponding to $\{x_{i,j}\}_{1 \leq i,j \leq r+1}$. As in Fig. 1, the vector $x_{i,j}$ stands for the cross point of the i -th row and the j -th column in the grid. The sum of all $r+1$ vectors in the same row (or the same column) is zero. Then for the coordinate (i, j) of \mathcal{C} where $1 \leq i, j \leq r+1$,

$$R_{row}^{(i,j)} = \{(i, 1), (i, 2), \dots, (i, r+1)\} \text{ and } R_{col}^{(i,j)} = \{(1, j), (2, j), \dots, (r+1, j)\}$$

are its two regenerating sets. Thus \mathcal{C} has $(r, \delta = 3)_c$ -locality, and therefore has locality $r^{(2)}$.

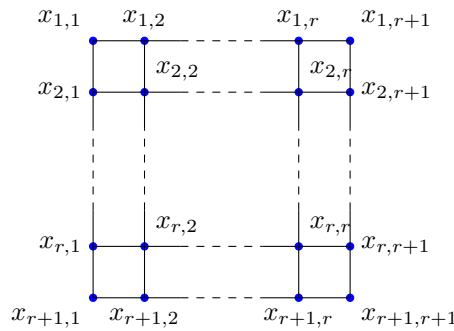


Fig. 1: The grid corresponding to vectors $\{x_{i,j}\}_{1 \leq i,j \leq r+1}$.

Next, we prove an upper bound on the minimum distance by using Theorem 1.

Theorem 5. *The minimum distance of a square code satisfies*

$$d \leq n - M + 1 - s,$$

where $s = \max\{x | g(x) < M\}$ and

$$g(x) = \begin{cases} xr - \frac{x^2}{4}, & \text{if } 2 \mid x \\ xr - \frac{x^2-1}{4}, & \text{if } 2 \nmid x \end{cases}$$

is a function defined over all integers x in the range $[0, 2r+1]$.

Proof: First, we prove that $\Phi(x) \leq g(x) + x$ for $0 \leq x \leq 2r+1$. In fact, observe that the $2r+1$ regenerating sets

$$R_{row}^{(1,r+1)}, R_{col}^{(r+1,1)}, R_{row}^{(2,r+1)}, R_{col}^{(r+1,2)}, \dots, R_{row}^{(r,r+1)}, R_{col}^{(r+1,r)}, R_{row}^{(r+1,r+1)}$$

have a nontrivial union (with respect to the order above). Thus for $0 \leq x \leq 2r+1$, $\Phi(x)$ is no more than the size of the first x regenerating sets' union which equals the function value $g(x) + x$. Consequently, we have $\Phi(x) \leq g(x) + x$.

Assume $s \geq \rho + 1$, then by the definition of ρ and the increasing property of $\Phi(x)$, it follows that

$$M \leq \Phi(\rho + 1) - (\rho + 1) \leq \Phi(s) - s \leq g(s),$$

which contradicts the definition of s . Therefore $\rho \geq s$ and Theorem 1 gives the desired bound. \blacksquare

In particular, the square code has $(r, \delta)_c$ -locality, so it also satisfies the upper bound in Theorem 4. But a comparison shows the bound in Theorem 5 is more precise for the square code in general. As an example, Fig. 2 displays the two bounds for the square code with $r = 5$.

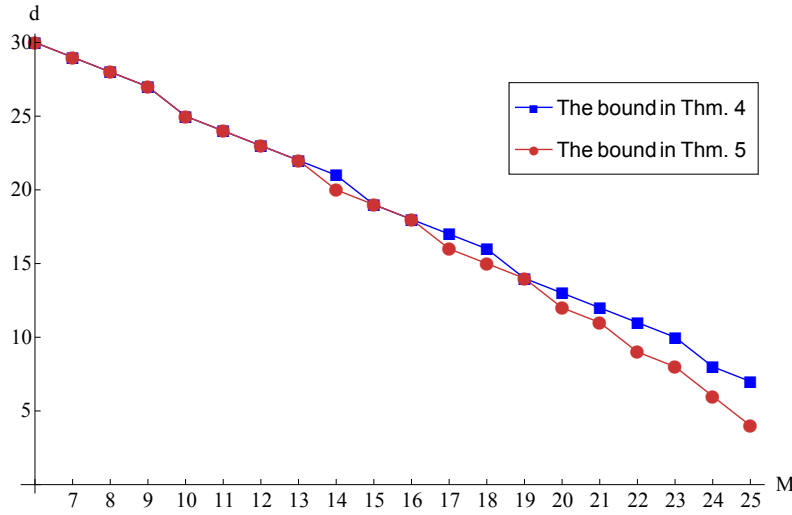


Fig. 2: The minimum distance upper bound for square codes with $r = 5$.

A. Construction of square codes with optimal distance

We present an explicit construction of the square code that has the minimum distance $d = n - M + 1 - s$, showing tightness of the upper bound given in Theorem 5.

Let \mathbb{F}_{q^m} be an extension field of \mathbb{F}_q , where $m \geq r^2$. Note that \mathbb{F}_{q^m} can be regarded as an m -dimensional linear space over \mathbb{F}_q . Then there exist r^2 elements $\{\beta_{i,j}\}_{1 \leq i,j \leq r}$ in \mathbb{F}_{q^m} that are linearly independent over \mathbb{F}_q . Moreover, let

$$\beta_{r+1,j} = - \sum_{i=1}^r \beta_{i,j} \text{ for } 1 \leq j \leq r$$

and

$$\beta_{i,r+1} = - \sum_{j=1}^r \beta_{i,j} \text{ for } 1 \leq i \leq r+1.$$

Let \mathcal{C} be an $(n, (M, 1), d)$ linear code over \mathbb{F}_{q^M} with generator matrix $G = (g_{i,j})_{1 \leq i, j \leq r+1}$, where $n = (r+1)^2$, $r+1 \leq M \leq r^2$ and

$$g_{i,j} = \begin{pmatrix} \beta_{i,j} \\ \beta_{i,j}^q \\ \vdots \\ \beta_{i,j}^{q^{M-1}} \end{pmatrix}.$$

Then \mathcal{C} is a square code of locality $r^{(2)}$ because

$$\sum_{i=1}^{r+1} g_{i,j} = \begin{pmatrix} \sum_{i=1}^{r+1} \beta_{i,j} \\ \vdots \\ \sum_{i=1}^{r+1} \beta_{i,j}^{q^{M-1}} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{r+1} \beta_{i,j} \\ \vdots \\ (\sum_{i=1}^{r+1} \beta_{i,j})^{q^{M-1}} \end{pmatrix} = 0, \text{ for } 1 \leq j \leq r+1$$

and similarly, $\sum_{j=1}^{r+1} g_{i,j} = 0$ for $1 \leq i \leq r+1$.

Next we show the minimum distance of \mathcal{C} satisfies $d \geq n - M + 1 - s$. Firstly, we quote a basic result of finite fields.

Lemma 4 ([5]). *Suppose $x_1, \dots, x_M \in \mathbb{F}_{q^M}$ are linearly independent over \mathbb{F}_q , then*

$$\det \begin{pmatrix} x_1 & x_2 & \cdots & x_M \\ x_1^q & x_2^q & \cdots & x_M^q \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{q^{M-1}} & x_2^{q^{M-1}} & \cdots & x_M^{q^{M-1}} \end{pmatrix} \neq 0.$$

Let S_1, \dots, S_{r+1} be a partition of $\{(i, j)\}_{1 \leq i, j \leq r+1}$, where $S_i = \{(i, j)\}_{1 \leq j \leq r+1}$ for $1 \leq i \leq r+1$.

Lemma 5. *Suppose X is a subset of $\{(i, j)\}_{1 \leq i, j \leq r+1}$ such that*

- (1) $|X| \geq M$ and $|X \cap S_i| \leq r$ for all $1 \leq i \leq r+1$.
- (2) there exists $1 \leq i_0 \leq r+1$ such that $X \cap S_{i_0} = \emptyset$.

Then $\text{rank}(G|_X) = M$.

Proof: The proof is based on Lemma 4. Let X' be a subset of X with size M . It is clear X' also satisfies the condition (1) and (2) in Lemma 5. Next, we prove that $\text{rank}(G|_{X'}) = M$. By Lemma 4, it suffices to show the M elements $\{\beta_{i,j}\}_{(i,j) \in X'}$ are linearly independent over \mathbb{F}_q .

For $1 \leq i \leq r+1$, let V_i be the linear space spanned by $\{\beta_{i,j}\}_{(i,j) \in S_i}$ over \mathbb{F}_q and let V be the space spanned by $\{\beta_{i,j}\}_{1 \leq i, j \leq r+1}$ over \mathbb{F}_q . Because of the choice of $\beta_{i,j}$, the sum of any r out of the $r+1$ spaces $\{V_i\}_{1 \leq i \leq r+1}$ is equal to V . Note that $\dim(V) = r^2$ and $\dim(V_i) = r$ for $1 \leq i \leq r+1$. It follows that V is the direct sum of any r subspaces out of $\{V_i\}_{1 \leq i \leq r+1}$. Particularly,

$$V = \bigoplus_{\substack{i=1 \\ i \neq i_0}}^{r+1} V_i. \quad (2)$$

On the other hand, for $1 \leq i \neq i_0 \leq r+1$, the condition $|X \cap S_i| \leq r$ implies that $\{\beta_{i,j}\}_{(i,j) \in X \cap S_i}$ are linearly independent over \mathbb{F}_q . Therefore $\{\beta_{i,j}\}_{(i,j) \in X'}$ are linearly independent over \mathbb{F}_q . \blacksquare

Theorem 6. *Let \mathcal{C} be the square code defined by the generator matrix $G = (g_{i,j})_{1 \leq i, j \leq r+1}$. Then*

$$d \geq n - M + 1 - s.$$

Proof: Assume on the contrary that $d \leq n - M - s$. Then there is a subset $N \subseteq \{(i, j)\}_{1 \leq i, j \leq r+1}$ such that $|N| = M + s$ and $\text{rank}(G|_N) < M$.

Let $N \cap S_i = N_i$, then $N = N_1 \cup \dots \cup N_{r+1}$ is a partition of N . Suppose that $a = \min\{|N_i| : 1 \leq i \leq r+1\}$ and b is the number of N_i 's such that $|N_i| = r+1$. Then clearly $a + b < 2r + 1$ and

$$\begin{aligned} |N| &= M + s \\ &= |N_1| + \dots + |N_{r+1}| \\ &\geq (r+1)b + (r+1-a)b \\ &= (r+1)(a+b) - ab. \end{aligned} \tag{3}$$

We claim that $s \geq a + b$ because otherwise, it has $s + 1 \leq a + b < 2r + 1$ which leads to

$$\begin{aligned} g(s+1) &\leq g(a+b) \\ &\leq r(a+b) - ab \\ &\leq M + s - (a+b) \\ &\leq M - 1, \end{aligned}$$

where the first inequality is due to increasing property of the function $g(x)$, the second comes from the fact that

$$ab \leq \begin{cases} \frac{(a+b)^2}{4}, & \text{if } a+b \text{ even} \\ \frac{(a+b)^2-1}{4}, & \text{if } a+b \text{ odd,} \end{cases}$$

the third is from (3) and the last is from the assumption $s + 1 \leq a + b$. But $g(s+1) \leq M - 1$ contradicts the definition of s . Therefore, $s \geq a + b$.

Suppose the b sets of size $r+1$ are N_{i_1}, \dots, N_{i_b} and N_{i_0} is a set of size a . Then delete one element in each of N_{i_1}, \dots, N_{i_b} and further delete N_{i_0} from N , we get a subset of N , denoted as \tilde{N} . It is clear that $|\tilde{N} \cap S_i| \leq r$ for $1 \leq i \leq r+1$ and $\tilde{N} \cap S_{i_0} = \emptyset$. Additionally, $|\tilde{N}| = |N| - (a+b) \geq M$ because $|N| = M + s$ and $s \geq a + b$. By Lemma 5, $\text{rank}(G|_N) \geq \text{rank}(G|_{\tilde{N}}) = M$, which contradicts the choice of N . ■

V. CONCLUSION

We introduce the regenerating set which can be used to characterize the local repair groups of any locally repairable codes. A connection between the regenerating set and the minimum distance is established. Under the framework of regenerating sets, we derive more general definition, more uniform and brief proofs, and more precise bound. This framework are expected to provide deeper insight into the design of locally repairable codes.

REFERENCES

- [1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. on Inform. Theory*, vol. 56, no. 9, pp. 4539C4551, 2010.
- [2] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. on Inform. Theory*, vol. 58, no.11, pp. 6925 - 6934, 2012.
- [3] C. Huang, M. Chen, and J. Li, "Pyramid codes: flexible schemes to trade space for access efficiency in reliable data storage systems", in *Proc. IEEE International Symposium on Network Computing and Applications (NCA 2007)*, Cambridge, MA, Jul. 2007.
- [4] O. Khan, R. Burns, J. Plank, and C. Huang, "In search of I/O-optimal recovery from disk failures," in *Hot Storage 2011, 3rd Workshop on Hot Topics in Storage and File Systems*, Portland, OR, Jun., 2011.
- [5] R. Lidl and H. Niederreiter, "Finite fields." Cambridge University Press, 1997.
- [6] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error Correcting Codes," North-Holland, 1977.
- [7] F. Oggier and A. Datta, "Self-repairing homomorphic codes for distributed storage systems," in *INFOCOM, 2011 Proceedings IEEE*, pp. 1215–1223, IEEE, 2011.
- [8] L. Pamies-Juarez, H. D. L. Hollmann, and F. Oggier. "Locally Repairable Codes with Multiple Repair Alternatives." in *Proc. of IEEE ISIT*, July, 2013.

- [9] D. S. Papailiopoulos, and A. G. Dimakis. "Locally repairable codes." in Proc. of IEEE ISIT, July, 2012.
- [10] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, "Optimal linear codes with a local-error-correction property," in Proc. of IEEE ISIT, July, 2012.
- [11] N. Silberstein, A. S. Rawat, O. O. Koyluoglu and S. Vishwanath "Optimal Locally Repairable Codes via Rank-Metric Codes." in Proc. of IEEE ISIT, July, 2013.
- [12] I. Tamo, D. S. Papailiopoulos, and A. G. Dimakis, "Optimal locally repairable codes and connections to matroid theory," in Proc. of IEEE ISIT, July, 2013.
- [13] I. Tamo, Z. Wang, and J. Bruck, "MDS array codes with optimal rebuilding," in Proc. of IEEE ISIT, Aug, 2011.
- [14] A. Wang and Z. Zhang. "Repair Locality with Multiple Erasure Tolerance." arXiv preprint arXiv:1306.4774 (2013).
- [15] H. Weatherspoon and J. D. Kubiatowicz, "Erasure coding vs. replication:a quantitative comparison," in Proc. IPTPS, 2002.